



Bitcoin

Bitcoin is a consensus network that enables a new payment system and a completely digital money. It is the first decentralized peer-to-peer payment network that is powered by its users with no central authority or middlemen. From a user perspective, Bitcoin is pretty much like cash for the Internet. Bitcoin can also be seen as the most prominent triple entry bookkeeping system in existence. Bitcoins are mathematically generated as the computers in this network execute difficult number crunching tasks, a procedure known as Bitcoin mining. The Mathematics of the Bitcoin system were set up so that it becomes progressively more difficult to mine bitcoins overtime and the total number that can ever be mined is limited to around 21 million.

Total bitcoins to be available	21,000,000
Top Bitcoin holders in the world	
Satoshi Nakamoto	1,000,000
MicroStrategy	92,079
Tesla	42,902
Galaxy Digital Holdings	16,400
Voyager Digital	12,260
Square	8,027

Creation

Bitcoin is the first implementation of a concept called "cryptocurrency", which was first described in 1998 by Wei Dai on the cypherpunks mailing list, suggesting the idea of a new form of money that uses cryptography to control its creation and transactions, rather than a central authority. The first Bitcoin specification and proof of concept was published in 2009 in a cryptography mailing list by Satoshi Nakamoto. Satoshi left the project in late 2010 without revealing much about himself. The community has since grown exponentially with many developers working on Bitcoin.

Satoshi's anonymity often raised unjustified concerns, many of which are linked to misunderstanding of the open-source nature of Bitcoin. The Bitcoin protocol and software are published openly and any developer around the world can review the code or make their own modified version of the Bitcoin software. Just like current developers, Satoshi's influence was limited to the changes he made being adopted by others and therefore he did not control Bitcoin. As such, the identity of Bitcoin's inventor is probably as relevant today as the identity of the person who invented paper.

The network

Nobody owns the Bitcoin network much like no one owns the technology behind email. Bitcoin is controlled by all Bitcoin users around the world. While developers are improving the software, they can't force a change in the Bitcoin protocol because all users are free to choose what software and version they use. In order to stay compatible with each other, all users need to use software complying with the same rules. Bitcoin can only work correctly with a complete consensus among all users. Therefore, all users and developers have a strong incentive to protect this consensus.

The program

From a user perspective, Bitcoin is nothing more than a mobile app or computer program that provides a personal Bitcoin wallet and allows a user to send and receive bitcoins with them. This is how Bitcoin works for most users. Behind the scenes, the Bitcoin network is sharing a public ledger called the "block chain". This ledger contains every transaction ever processed, allowing a user's computer to verify the validity of each transaction. The authenticity of each transaction is protected by digital signatures corresponding to the sending addresses, allowing all users to have full control over sending bitcoins from their own Bitcoin addresses. In addition, anyone can process transactions using the computing power of specialized hardware and earn a reward in bitcoins for this service. This is often called "mining". To learn more about Bitcoin, you can consult the dedicated page and the original paper.

Is Bitcoin really used by people?

Yes. There are a growing number of businesses and individuals using Bitcoin. This includes brick-and-mortar businesses like automobile, hotels, restaurants, apartments, and law firms, as well as popular online services such as Namecheap and Overstock.com. While Bitcoin remains a relatively new phenomenon, it is growing fast. As of 4 august 2021, the total value of all existing bitcoins exceeded 740 billion US dollars, with millions of dollars' worth of bitcoins exchanged daily.

How does one acquire bitcoins?

- As payment for goods or services.
- Purchase bitcoins at a Bitcoin exchange.
- Exchange bitcoins with someone near you.
- Earn bitcoins through competitive mining.

While it may be possible to find individuals, who wish to sell bitcoins in exchange for a credit card or PayPal payment, most exchanges do not allow funding via these payment methods. This is due to cases where someone buys bitcoins with PayPal, and then reverses their half of the transaction. This is commonly referred to as a chargeback.

Payment system

Bitcoin payments are easier to make than debit or credit card purchases and can be received without a merchant account. Payments are made from a wallet application, either on your computer or smartphone, by entering the recipient's address, the payment amount, and pressing send. To make it easier to enter a recipient's address, many wallets can obtain the address by scanning a QR code or touching two phones together with NFC technology.

Merits of Bitcoin?

Payment freedom - It is possible to send and receive bitcoins anywhere in the world at any time. No bank holidays. No borders. No bureaucracy. Bitcoin allows its users to be in full control of their money.

Choose your own fees - There is no fee to receive bitcoins, and many wallets let you control how large a fee to pay when spending. Higher fees can encourage faster confirmation of your transactions. Fees are unrelated to the amount transferred, so it's possible to send 100,000 bitcoins for the same fee it costs to send 1 bitcoin. Additionally, merchant processors exist to assist merchants in processing transactions, converting bitcoins to fiat currency and depositing funds directly into merchants' bank accounts daily. As these services are based on Bitcoin, they can be offered for much lower fees than with PayPal or credit card networks.

Fewer risks for merchants - Bitcoin transactions are secure, irreversible, and do not contain customers' sensitive or personal information. This protects merchants from losses caused by fraud or fraudulent chargebacks, and there is no need for PCI compliance. Merchants can easily expand to new markets where either credit cards are not available, or fraud rates are unacceptably high. The net results are lower fees, larger markets, and fewer administrative costs.

Security and control - Bitcoin users are in full control of their transactions; it is impossible for merchants to force unwanted or unnoticed charges as can happen with other payment methods. Bitcoin payments can be made without personal information tied to the transaction. This offers strong protection against identity theft. Bitcoin users can also protect their money with backup and encryption.

Transparent and neutral - All information concerning the Bitcoin money supply itself is readily available on the block chain for anybody to verify and use in real-time. No individual or organization can control or manipulate the Bitcoin protocol because it is cryptographically secure. This allows the core of Bitcoin to be trusted for being completely neutral, transparent, and predictable.

Demerits of Bitcoin

Degree of acceptance - Many people are still unaware of Bitcoin. Every day, more businesses accept bitcoins because they want the advantages of doing so, but the list remains small and still needs to grow in order to benefit from network effects.

Volatility - The total value of bitcoins in circulation and the number of businesses using Bitcoin are still very small compared to what they could be. Therefore, relatively small events, trades, or business activities can significantly affect the price. In theory, this volatility will decrease as Bitcoin markets and the technology matures. Never before has the world seen a start-up currency, so it is truly difficult (and exciting) to imagine how it will play out.

Ongoing development - Bitcoin software is still in beta with many incomplete features in active development. New tools, features, and services are being developed to make Bitcoin more secure and accessible to the masses. Some of these are still not ready for everyone. Most Bitcoin businesses are new and still offer no insurance. In general, Bitcoin is still in the process of maturing.

Bitcoin Trustworthiness

Much of the trust in Bitcoin comes from the fact that it requires no trust at all. Bitcoin is fully open-source and decentralized. This means that anyone has access to the entire source code at any time. Any developer in the world can therefore verify exactly how Bitcoin works. All transactions and bitcoins issued into existence can be transparently consulted in real-time by anyone. All payments can be made without reliance on a third party and the whole system is protected by heavily peer-reviewed cryptographic algorithms like those used for online banking. No organization or individual can control Bitcoin, and the network remains secure even if not all of its users can be trusted.

Money Multiplier

You should never expect to get rich with Bitcoin or any emerging technology. It is always important to be wary of anything that sounds too good to be true or disobeys basic economic rules.

Bitcoin is a growing space of innovation and there are business opportunities that also include risks. There is no guarantee that Bitcoin will continue to grow even though it has developed at a very fast rate so far. Investing time and resources on anything related to Bitcoin requires entrepreneurship. There are various ways to make money with Bitcoin such as mining, speculation or running new businesses. All of these methods are competitive and there is no guarantee of profit. It is up to each individual to make a proper evaluation of the costs and the risks involved in any such project.

Is Bitcoin fully virtual and immaterial?

Bitcoin is as virtual as the credit cards and online banking networks people use every day. Bitcoin can be used to pay online and in physical stores just like any other form of money. Bitcoins can also be exchanged in physical form such as the Denarium coins but paying with a mobile phone usually remains more convenient. Bitcoin balances are stored in a large, distributed network, and they cannot be fraudulently altered by anybody. In other words, Bitcoin users have exclusive control over their funds and bitcoins cannot vanish just because they are virtual.

Is it anonymous?

Bitcoin is designed to allow its users to send and receive payments with an acceptable level of privacy as well as any other form of money. However, Bitcoin is not anonymous and cannot offer the same level of privacy as cash. The use of Bitcoin leaves extensive public records. Various mechanisms exist to protect users' privacy, and more are in development. However, there is still work to be done before these features are used correctly by most Bitcoin users.

Some concerns have been raised that private transactions could be used for illegal purposes with Bitcoin. However, it is worth noting that Bitcoin will undoubtedly be subjected to similar regulations that are already in place inside existing financial systems. Bitcoin cannot be more anonymous than cash and it is not likely to prevent criminal investigations from being conducted. Additionally, Bitcoin is also designed to prevent a large range of financial crimes.

What happens when bitcoins are lost?

When a user loses his wallet, it has the effect of removing money out of circulation. Lost bitcoins still remain in the block chain just like any other bitcoins. However, lost bitcoins remain dormant forever because there is no way for anybody to find the private key(s) that would allow them to be spent again. Because of the law of supply and demand, when fewer bitcoins are available, the ones that are left will be in higher demand and increase in value to compensate.

Scale to become a major payment network

The Bitcoin network can already process a much higher number of transactions per second than it does today. It is, however, not entirely ready to scale to the level of major credit card networks. Work is underway to lift current limitations, and future requirements are well known. Since inception, every aspect of the Bitcoin network has been in a continuous process of maturation, optimization, and specialization, and it should be expected to remain that way for some years to come. As traffic grows, more Bitcoin users may use lightweight clients, and full network nodes may become a more specialized service. For more details, see the Scalability page on the Wiki.

Source:

<https://bitcoin.org/en/faq#what-if-someone-bought-up-all-the-existing-bitcoins>

If you are interested in discussing crypto assets or adding them to your portfolio, please feel free to call me at 215-325-1595 or set an appointment to talk using this link [Click here to schedule a meeting](#).

Broadhurst Financial Advisors now has the ability to add a small (1 to 5%) allocation of this new and unique asset class to your portfolios for the clients that are interested in adding more diversification and potential return to their holdings.



Jeffrey Broadhurst
MBA, CFA, CFP
Broadhurst Financial Advisors, Inc.



****PRIVACY NOTICE****

This message is intended only for the individual or entity to which it is addressed and may contain information that is privileged, confidential, or exempt from disclosure under applicable federal or state law. You are hereby notified that any dissemination, distribution, or copying of this communication, except in accordance with its intended purpose, is strictly prohibited.

Our emailing address:
1911 W Point Pike, POB 301
PA 19486, United States

Contact us:
Phone: (215) 325-1595
Email: jeff@broadhurstfinancial.com